symmetry

MDPI

Article

M2M Security Technology of CPS Based on Blockchains

Shiyong Yin [1], Jinsong Bao [1,*], Yiming Zhang [2] and Xiaodi Huang [3]

[1] College of Mechanical Engineering, Donghua University, Shanghai 201620, China; ycfysjk@126.com
[2] College of Literature, Science and the Arts, The University of Michigan, Ann Arbor, MI 48109, USA; yimingz@umich.edu
[3] School of Computing and Mathematics, Charles Sturt University, Albury NSW 2640, Australia; xhuang@csu.edu.au
* Correspondence: Bao@dhu.edu.cn; Tel.: +86-216-779-2562

Received: 24 August 2017; Accepted: 12 September 2017; Published: 14 September 2017

Abstract: As the core of intelligent manufacturing, cyber-physical systems (CPS) have serious security issues, especially for the communication security of their terminal machine-to-machine (M2M) communications. In this paper, blockchain technology is introduced to address such a security problem of communications between different types of machines in the CPS. According to the principles of blockchain technology, we designed a blockchain for secure M2M communications. As a communication system, M2M consists of public network areas, device areas, and private areas, and we designed a sophisticated blockchain structure between the public area and private area. For validating our design, we took cotton spinning production as a case study to demonstrate our solution to M2M communication problems under the CPS framework. We have demonstrated that the blockchain technology can effectively solve the safety of expansion of machines in the production process and the communication data between the machines cannot be tampered with.

Keywords: blockchain; machine-to-machine (M2M); cyber-physical system (CPS); cotton spinning production

1. Introduction

A cyber-physical system (CPS) is a complex system of computation, networks, and the physical world [1]. By using computing, communication, and control technologies, a CPS digitizes the physical world and realizes the unity of the information world and the physical world. Typically, a CPS consists of two main parts: one is the physical world, while another is an information system. Aiming to mine and analyse data of the physical world from the information world, a CPS intelligently monitors actions of entities in the physical world, and takes actions to change their behaviour to make the entities work more efficient. As a dynamic network, the industrial Internet of Things (IIoT) has physical and virtual bodies with its own identities and properties. It uses a smart interface to connect a physical world with a virtual world [2]. Relying on a variety of technologies, including sensing, communication, computing, data processing, and feedback control technology, machine-to-machine (M2M) supports intercommunication of many heterogeneous devices [3]. Nowadays, M2M has become an indispensable part in the next-generation network, and is being widely applied to many new smart applications and services. As the epoch of Industry 4.0 approaches, CPS, IIoT, and M2M have been infiltrating the industry.

Current M2M security protocols are not capable of resolving the intercommunications between different heterogeneous devices in CPS devices. How to ensure the safety of communication of M2M is a question that is in urgent need of being solved. This paper attempts to solve the security of M2M in a CPS using blockchain technology. The main contributions of this work are as follows: (1) blockchain

technology to solve the security problems of M2M communication is introduced; (2) the design of a blockchain for M2M communication security is presented; and (3) the application of blockchain technology to a case study of cotton spinning is given.

The rest of this paper is organized as follows: Section 2 presents related work. Section 3 introduces the blockchain technology. It mainly presents the connotation and characteristics of the blockchain, the nature of the blockchain, and its core technology. Afterwards, the safer M2M communication with the help of blockchain technology is discussed. Section 4 presents our blockchain design, including the design of the overall structure, the public network area blockchain, and private area blockchain. Section 5 describes a case study where we apply blockchain technology into the M2M communication of an intelligent cotton production CPS to solve malleability and instant security issues of an M2M system. Finally, Section 6 concludes this paper.

2. Related Work

With the in-depth development and applications of CPS, its security issues increasingly become a concern. Related security issues are broadly studied and analysed in the fields of wireless sensor network, ad hoc network, and mobile ad hoc networks. They are, however, barely applicable. This is because CPS security covers a larger scope, contains much more content and requires higher levels of security. Security issues are not new. We should use advances in technology to address this issue. An analysis of the security issues at the various layers of the CPS architecture, risk assessment, and techniques were discussed for securing CPS in [4]. A framework for modelling the security of a cyber-physical system has been described [5], where the behaviour of the adversary is controlled by a threat model that captures the cyber aspects and the physical aspects of the cyber-physical system in a unified manner. Moreover, a content-aware security framework for generic CPS systems has been proposed [6], together with an investigation of the CPS security issues. Several security problems along with the currently proposed solutions at different network layers of mobile ad hoc networks have been discussed as well [7]. Through applications of current network security models to a CPS, flaws in the original model have been found. In response to this, a new model was proposed to address the challenges of CPS security [8]. The security design of the IoT should be standardized to achieve an open, widespread, and interacting fundamental security architecture [9]. On the basis of investigations of CPS security, the authors of [10] presented a series of challenges that urgently needed to be resolved to boost the performance of the CPS. A modelling approach to evaluating the security of a CPS was then presented, in which a game-theoretic paradigm with different parameters predicted the interactions between the attacker and the system [11]. Any leakage of private information in a CPS will cause serious consequences. Enhancing the secrecy of wireless communications in a CPS by using physical layer security techniques is key. A privacy-enhanced waveform design approach aided by artificial noise has been proposed to enhance the communication secrecy in a wireless environment with multipath reception [12]. Some security issues that may occur in a CPS have also been discussed [13,14].

A vast number of M2M intelligent devices have been deployed in CPSs. Thus, the security of M2M determines the performance of the CPS. A simplified protocol stack has been proposed, and some important sections introduced, to provide secure transmission between M2M servers and their terminals [15]. In [16], a survey of security threats against M2M network solutions to prevent or reduce their impact was presented after an overview of potential M2M applications was provided [16]. M2M communication faces a large number of security threats. For some unresolved security vulnerabilities, a dynamic-encryption authentication scheme has been proposed, by which a mobile device could be authenticated by the network and a shared one-time-password could be generated. It can withstand man-in-the-middle attacks, impersonation attacks, reply attacks, and disk operation system (DOS) attacks [17]. Distributing trust building and enforcement tasks between devices and networks leads to scalable concepts, which can provide a flexible solution to new threats that arise in M2M communications [18]. Combined with M2M characteristics, an improved direct anonymous

authentication scheme has been proposed [19]. To prevent accidents, the design of an environmental monitoring platform of mines based on M2M technologies has also been proposed [20]. In [21], after discussing the security challenges in M2M communications in the wireless networks of CPSs, a secure architecture that is suitable for CPSs was proposed to cope with these security issues. Four aspects of the corresponding countermeasures to these security issues were discussed: access control, intrusion detection, authentication, and privacy preserving, respectively. Providing real-time cloud services to vehicular clients must address delay and delay-jitter issues. An energy-efficient adaptive resource scheduler for networked fog centres was reported with the test results [22]. The use of peer-to-peer (P2P) grid technology allows for the creation of a network with greater distribution and scalability. A reputation model on trust management is proposed for a semantic P2P grid, which can achieve good computational complexity with high ranking accuracy [23]. Harnessing the broadcast nature of wireless channels towards efficient multicast faces challenging security issues. For improving security in a wireless multicast, a dynamic fountain code was designed against passive eavesdropping [24]. It can significantly reduce the intercepting probability while achieving a higher transmission efficiency, thus facilitating wireless connections in support of multicast services.

A number of frameworks and proposals on M2M security are available. To the best of our knowledge, this work is, however, the first attempt to apply blockchain technology into M2M communication security in a real-world case study.

3. Blockchain Technology

3.1. The Connotation and Main Features of a Blockchain

After the inventor of Bitcoin published a paper named "Bitcoin: A peer-to-peer electronic cash system" [25] in 2008, blockchain saw significant publicity. Later, Swan claimed that blockchain is a transparent distributed database [26]. The Ministry of Industry and Information technology of the People's Republic of China defines a blockchain as a creative application of distributed storage, P2P transmission, consensus mechanisms, and encrypted algorithms. Despite being far from reaching consensus on the definition of a blockchain, the connotation is fairly clear. Using mathematics as its foundation, a blockchain is a multidisciplinary technology that also combines cryptography, economic models, and network technology into a distributed system that is established on distrust and indecent operations. The main features of a blockchain are as follows:

(1) Rather than creating a system around a central server, blockchain utilizes P2P networking and a consensus mechanism to create the trust system between nodes, thus forming a decentralized system.
(2) A blockchain uses encryption, especially asymmetrical encryption, to protect transaction data. A consensus mechanism ensures that data cannot be modified or forged, guaranteeing a high level of security.
(3) Based on the chain structure, all data of a transaction are traceable. A blockchain utilizes special methods to motivate all nodes to cooperate in block verification and uses a consensus mechanism to choose specific nodes as new blocks [27].

3.2. The Working Mechanisms of a Blockchain

3.2.1. The Structure of a Blockchain

A blockchain is an ordered chain of blocks. Blocks are containers of some related information and the data of transaction records. The different blocks may vary, but a normal block consists of a block head, which contains metadata, and a block body, which records the transaction process. The structure of a block is shown in Figure 1. A block head has three main parts, except for its version number: ① a hash value linked to the previous block, which is essential to the chain structure; ② a hash function, timestamp, and nonce related to transactions (hash functions are used to store blockchain data; a timestamp records the time at which blocks are generated; a nonce is a calculator used in proofs

of the work algorithm); ③ a Merkel root used to summarize all transactions in the block and to quickly check the existence and integrity of the transaction data. A block body stores all verified transactions during the generation of a block. By linking blocks with hash values, a blockchain is created.

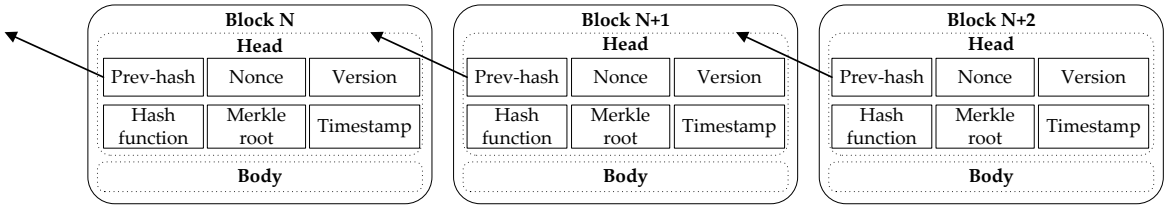

Figure 1. The structure of a blockchain.

3.2.2. The Working Principle of a Blockchain

The working principle of a blockchain is illustrated in Figure 2. In the bitcoin network, if A wants to send a bitcoin to B, the following processes will be followed: ① Create a transaction order. Encrypt the previous transaction with B's public key, calculate the hash value, and then encrypt the hash value with its own private key to obtain its digital signature, and finally add the digital signature to the end of the bitcoin to create a transaction order. ② Broadcast the transaction order. Broadcast the transaction order to the Internet to inform other nodes about the transaction and each node incorporates received the transaction into a block. ③ Verify transaction validity. All participants verify the validity of the transaction by searching for solution x, which allows the hashed value computed from x, the hash value of the last block of the blockchain, and the transaction order using the Hash256 algorithm satisfies certain conditions; for example, the first 20 digits are 0. After the solution is found, the privilege of creating a new block is guaranteed and a bitcoin is rewarded. ④ Transmit the verification results. The node that computes the solution firstly receives the bitcoin from the system and this piece of information is broadcast to all the nodes through the Internet. ⑤ Complete the transaction. A's and B's bitcoins are separately changed in the distributed ledger.

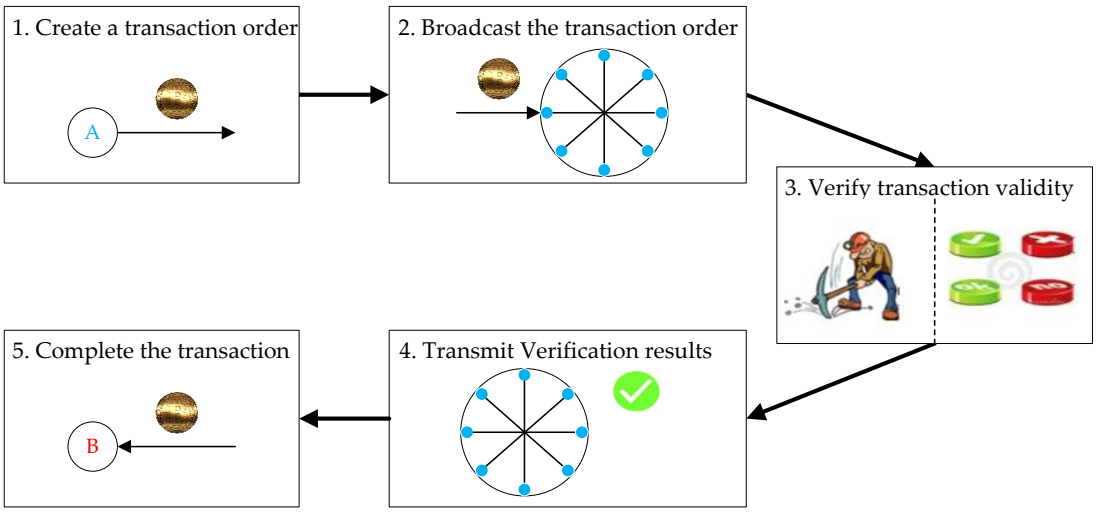

Figure 2. The working principle of a blockchain.

3.3. The Utilization of Blockchain for M2M Communication of CPS

Features of a blockchain and M2M communication of CPS are compatible to some extent. For example:

(1) Blockchain technology and M2M both utilize the idea of distributed and decentralized computing. There is no centralized database in a blockchain, with each network node storing its own copy of

the blockchain. The physical level of a CPS contains energy/environment, personnel, and various types of physical equipment and other elements. The interconnection between machines and equipment (M2M) is a key technology in a CPS, and it can take the form of machine-to-machine, machine-to-cluster, and even cluster-to-cluster. However, no matter which form the M2M takes, they all exhibit the same nature of decentralization.

(2) A blockchain and M2M both require high levels of security. Other than a system being built on dependency and trust, a blockchain uses encryption and digital signature to secure information. While in an M2M system, the transmission and storage of information also require high confidentiality, integrity and validity, and authenticity. In addition, M2M has the nature of non-repudiation. Despite some level of variation in different systems, for example, military, electrical, medical, and manufacturing systems, the security of information is generally the first priority of such systems.

(3) A blockchain and M2M reach a high level of harmony in the traceability and sharing of information. Providing effective sharing of historical information, blockchain technology uses a hash value, which is connected to the previous block, to track information of transactions throughout the whole blockchain. In M2M systems, especially in the area of manufacturing, tracing historical data is crucial. For instance, by reviewing data, we can identify key factors that might impact product quality. By improving processes, a higher quality will then be achieved. By filtering through the data, we can discover weak spots in production. The rate of machine breakdowns will then be lowered considerably by optimizing the maintenance methods. Additionally, through data sharing, those unnecessary processes can be easily spotted. Then cutting or reducing expenses of these processes on the supply chain will help cut production costs.

4. M2M-Security-Oriented Blockchain Design

4.1. Overall Design

On the foundation of ensuring data throughput and extensibility, to achieve validity of data, which means that data are usable, reliable, integral, safe, and manageable, senders of data are required to send real, legal, and standardized data. The transmission must be covert, recorded, queryable, and traceable. The receivers can only receive the data sent from the senders which cannot be forwarded. The process of receiving data can be recorded and queryable. In an M2M transmission system of CPS, the design of the blockchain in this work is illustrated in Figure 3.

(1) Public network area. Based on the industrial Internet of Things, the public network area builds machine communication platforms. This ensures the normal communication of various types of machines, audits the registration of machines, accesses authentication to achieve connection and communication among machines, unifies the data format and communication rules, maintains the blocks of the public network area, and queries communication records.

(2) Device area. The device area is the channel connecting the public network area and the private area. It receives messages from the public network area, and passes the query requests and query results to and from the private area.

(3) Private area. The private area establishes and records the blocks of communication process among machines, saves data of the communication process, accepts the external query, or obtains externally related data by querying.

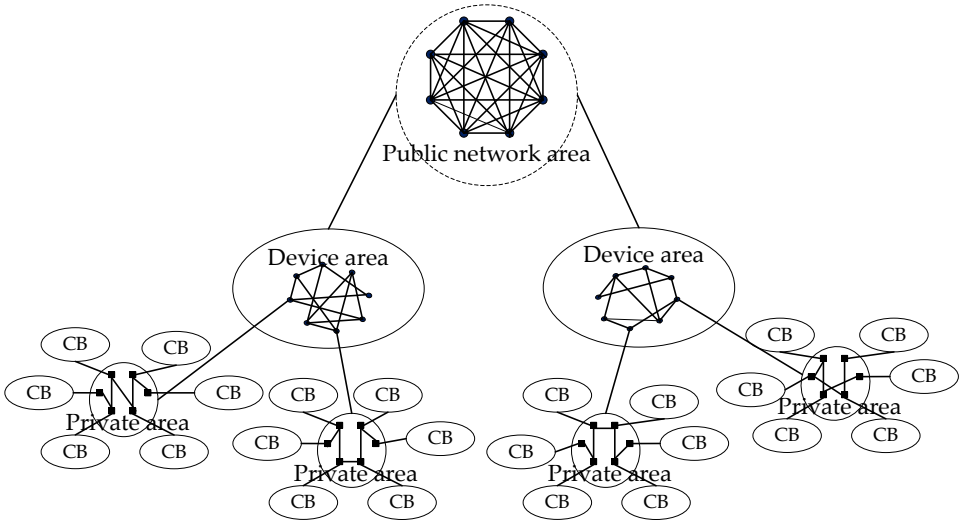

Figure 3. Our overall design of the blockchain for machine-to-machine (M2M) security.

4.2. Design of Machine-Equipment Blockchain in the Public Network Area

In a CPS, if devices must be replaced due to malfunctioning or other reasons, the new device will have to be connected to the production line by registration. The new device calculates a private key from a random number by using an algorithm such as the SHA256 algorithm [28], and then generates a public key by using another algorithm, such as the Secp256K1 algorithm [29]. In this way, a key pair is formed. The new device sends the digital certificate which marks its own identity together with the public key to the public network area for registration. It will be successfully registered after approval. Then, the public network will create an equivalence between the certificate and its identity, and store the public key of this device into the key pool. At the same time, the device is added as a new blockchain into the machine-equipment blockchain (M-EB). The structure of the M-EB is shown in Figure 4. After a public area has accepted and registered a new device, the M-EB will use the public key to verify the encrypted digital certificate, confirm the identity of the device, and finally authorize access into this area. Up until now, the new device can participate in M2M communication.

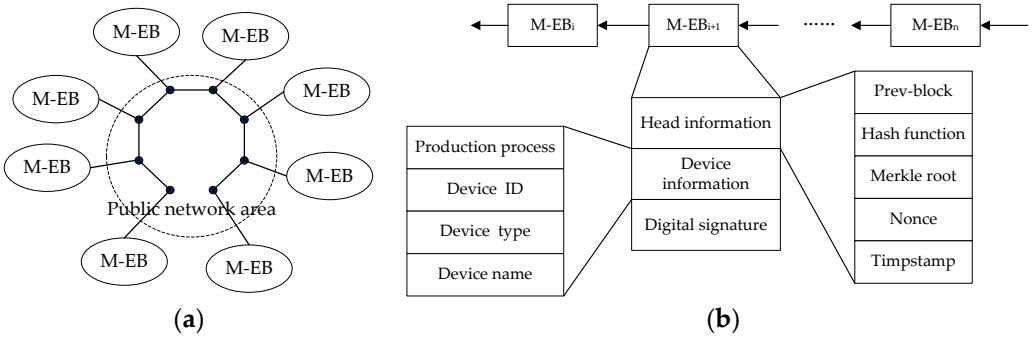

Figure 4. The design of the machine-equipment blockchain in public: (**a**) the schematic diagram of the machine-equipment blockchain in public network area; (**b**) the structure of the machine and equipment blockchain.

M2M technology uses a communication mechanism, which aims to empower all machines with the ability of communication, to realize the smart and interactive connections between machines and systems. To maintain data integrity and reduce data redundancy, the public network should standardize the format of communication among any M2M terminals of CPS. Here, we also reach a consensus on types of communication data: uploading information that refers to the collection of local

data, and downloading information that refers to the communication protocol, orders of networks, and settings of parameters.

4.3. Design of Communication Blockchain in the Private Area

Private sectors are in charge of recording communications between blocks, storing data, and querying the relevant information. Since information about the communication process can be shared, private sectors ensure that it is difficult to be tampered with.

The blocks of a communication blockchain (CB) are composed mainly of header information and communication information. In particular, header info includes: ① a hash value that links to the previous block, ② a target hash, ③ a Merkel root, ④ a nonce, ⑤ a timestamp, and other components. Communication information consists of ① a sender ID, to identify the initiator, ② receiver ID, to identify the receiver, ③ information type, to embody the data type of communication and tell whether it is uploaded data or downloaded data, ④ data size, to specify the total number of bytes of the data unit, ⑤ data, to be stored for specific communication data required, ⑥ encryption type, to specify the type of encryption, and ⑦ information verification, to verify the accuracy of the data after transmission. The structure of the communication blockchain is illustrated in Figure 5.

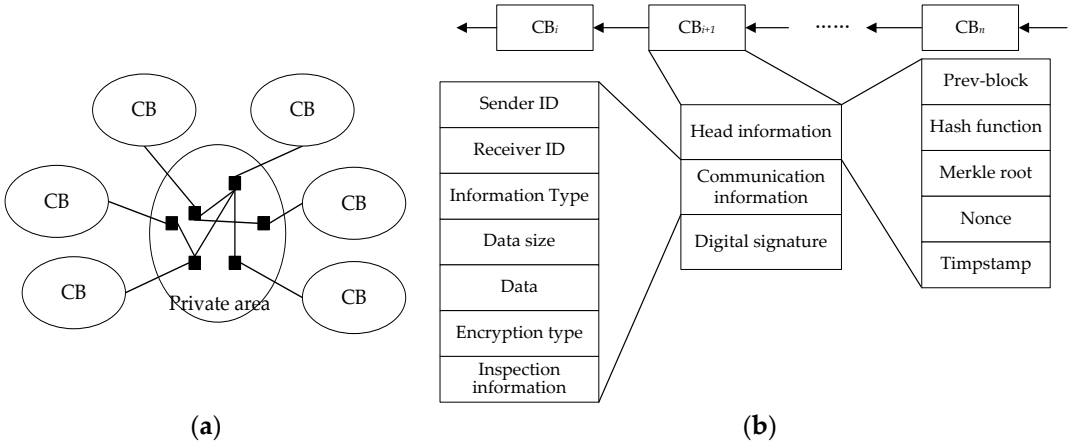

Figure 5. The design of the communication blockchain in the private area: (**a**) the schematic diagram of the communication blockchain in the private area; (**b**) the structure of the communication blockchain.

The communication blockchain mainly records the communications between devices. Each communication is linked to the blockchain as a separate block. The data in the interworking process, including the ID of the communication, the type of information, the size of the data, and the encryption mode, are saved to the block.

If device M1 wants to search for its communication record with a certain device, M2, for example, can send a query packet to the public network area in the form shown in Figure 6. If the query is successful, M2 returns the packet of the query result to M1 through the public network area. The format of the packet is shown in Figure 7. Otherwise, the public network area returns the query failure message back to M1.

Receiver ID	Sender ID	Digital signature of Sender	Data to be inquired	Inspection information

Figure 6. The data format of a query packet.

Receiver ID	Sender ID	Digital signature of Sender	Encrypted data	Inspection information

Figure 7. The data format of an information packet.

The whole process of query communication is illustrated in Figure 8. The step-by-step descriptions are detailed as follows:

Step 1: M1 sends a query packet to the public network area.

Step 2: After receiving the query packet, the public network area resolves the query packet and checks whether it is complete or not, according to the data check information. If not, M1 is required to resend the packet and the system re-enters Step 1; otherwise, the system enters Step 3.

Step 3: According to the ID of M2 in the query packet, the public network area checks whether M2 exists in the machine-equipment blockchain or not. If not, a null value from the public network area is sent to the query sender, and the query fails; otherwise, the system enters Step 4.

Step 4: The public network area delivers the query packet to the private area of M2 through the equipment sector.

Step 5: The private area of M2 analyses the query packet to decide if the digital signature of packet is legal. If not, the service request will be denied, and denial of service information will be sent to M1 through the public network area. The system re-enters Step 1; otherwise, it goes directly to Step 6.

Step 6: The private area of M2 searches for the query packet in the history. It encrypts the results using M1's public key and then encapsulates it into a packet, which is later sent to the public network area.

Step 7: After receiving the packet, the public network area checks whether or not it is complete according to the inspection information in the packet. If not, M2 is required to resend the packet; otherwise, the system goes to Step 8.

Step 8: The information packet is sent to the private area of M1 through its device area.

Step 9: The private area analyses the digital signature of M2 to identify its legitimacy. If it is illegal, M2 will be required to resend the packet and the system re-enters Step 6. Otherwise, the private area of M1 uses its private key to obtain the data and the whole query completes.

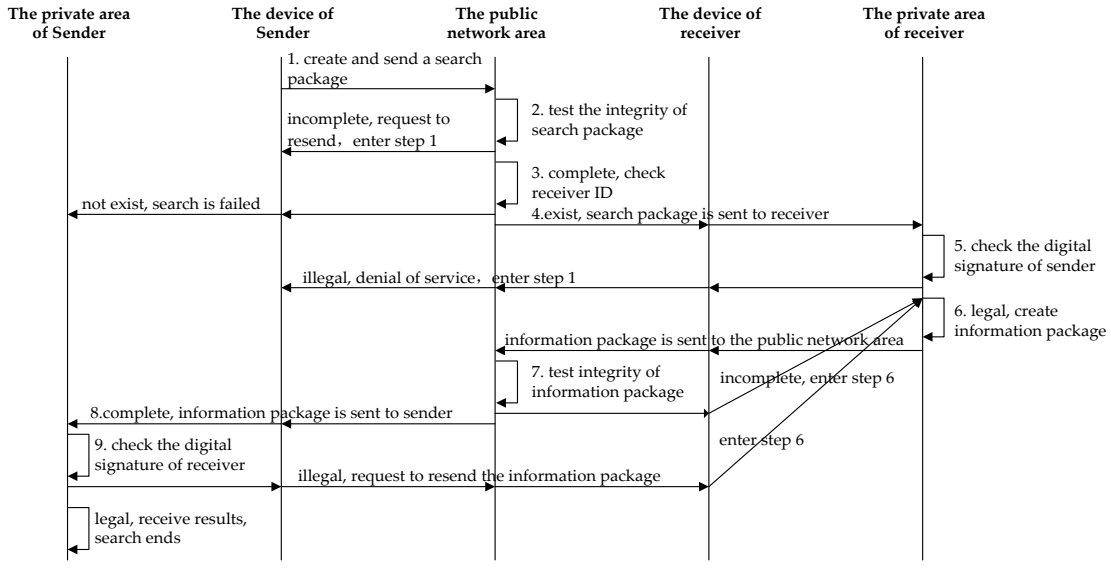

Figure 8. The communication process for a search.

5. A Case Study: Cotton-Production-Oriented Security of M2M under a CPS Architecture

In this section, we present a case study to exemplify our design of the Blockchain under a CSP architecture.

5.1. Problem Description

Traditional cotton production is quite a complicated process. As illustrated in Figure 9, cotton spinning involves a few key processes: blow room opening, cleaning, and mixing, carding, drawing, lap forming, combing, carded yarn, combed yarn, packing palletizing, etc. The processes are complex and continuity is demanded.

The cotton-production-oriented CPS architecture involves a bottom physics layer of machines, devices, energy, environment, and workers, and a middle layer of the industrial network based on various types of smart sensors, radio-frequency identification, WiFi, and tags. In our design, hundreds of high-performance sensors will need to be deployed in one single cotton production workshop to differentiate machines, equipment, or raw materials. By then, each device will record vast amounts of real-time data, e.g., quality data of cotton yarn during each processes and the status data of operational devices. As production proceeds, a cotton bale becomes cotton slivers, carded yarns, and, finally, combed yarns. The whole transformation process will also establish a great amount of data. Therefore, in the large data environment, intelligent cotton production will encounter the following challenges: First, though the size of cotton-production-oriented CPS is very large in size, M2M technology is increasingly mature, and the CPS itself is growing. Specifically, the equipment will increase or decrease in number according to the actual needs of production without sacrificing the stability of M2M communication. Second, if a carding machine sends a query request, for example, to a lap-forming machine laid on its previous process for information regarding the lap-forming status and quality so as to adjust its own setting accordingly, the M2M system will then have to send an instruction to extend the working hours to the related machines, due to the sudden increase of the order quantity. A carding machine also conveys quality information of carded yarn to the combing machine as a reference to adjust a proper parameter. How can this information or these instructions be transmitted safely to its target device? By answering this question, this case study discusses how to ensure communication scalability in the dynamic change of the M2M system under the CPS architecture for cotton spinning and timeliness and safety of multipoint-to-multipoint communication in the data environment.

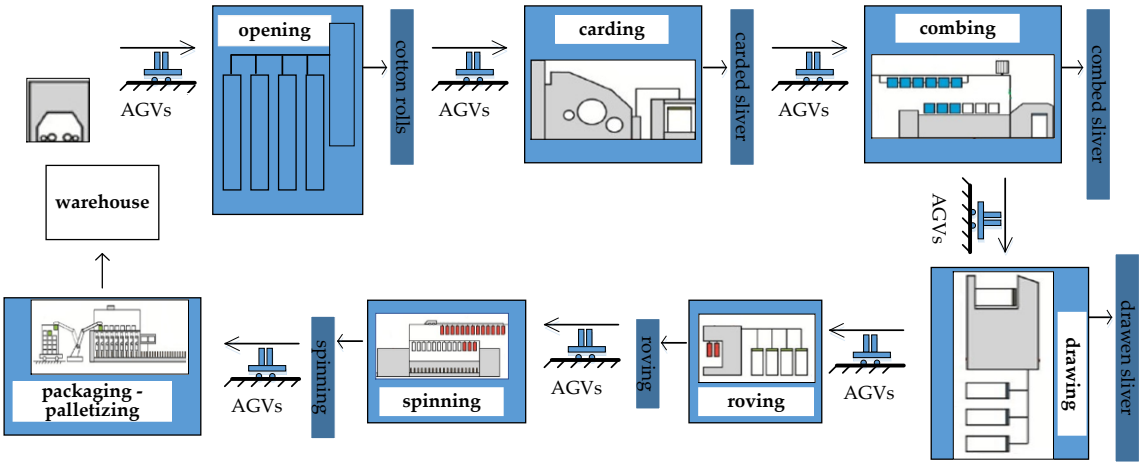

Figure 9. The process flow diagram of cotton spinning.

5.2. Solution and Simulations

In this section, we present our solution to the cotton-production-oriented security of M2M, together with the simulations that validate our design.

We conducted the simulations by the selecting the Enterprise 2015 version of C# language developed by Microsoft. The reasons for this are as follows: (1) The NET framework is popular, and we can create a portable code that functions across iOS, Android, Windows tablets/phones, desktops, servers, and embedded systems; (2) everything from the compiler to the core runtime is open source.

The program is executed with the following environment: Windows 10, Intel (R) Core™ i5-5200U 2.20 GHz CPU, and 8.0 GB of RAM.

The application types of C# mainly include Windows console applications, Windows form applications, ASP.NET Web applications, and ASP.NET Web services applications. We chose Windows console application programming by which to implement our simulation in this work. Console applications typically use standard command-line inputs and outputs. The information in the blockchain is handled with the combination of the bitcoin class.

Our simulation is implemented by using C#. There are four kinds of information flows in the simulation, namely, the material blockchain, the device blockchain, the communication blockchain, and the control flow of the program itself. The Merkel class of the blockchain can read and write blockchain information directly.

In the C# environment, the output of the model has two classes of request and confirms to apply to a user for help using the information in the blockchain. The request class and confirm class contain the Merkel roots of the latest block. The user sends a request message, waiting for a fixed cycle time in order to receive the confirmation message. Once the user receives the confirmation message, the method of processing the information starts to execute the output. If the output is the query information, the output is executed before being processed by two classes: query request and query results return.

5.2.1. Maintenance of Extensibility of M2M

If a production line is built, new devices must be added to the industrial network. Things will happen when the production line has to be modified or updated according to needs. Some devices must be substituted. In a word, M2M systems are dynamic and must be extensible. How, then, does one maintain the extensibility of M2M systems?

M2M systems of a CPS use blockchain technology to maintain extensibility. Industrial IoT platforms recognize the IDs of new devices and timestamps them before adding them to the blockchain as a new block (see Figure 10). For a changing scenario, the information of the replaced parts are still stored in the equipment blockchain as historical data for later querying and analysing. If a large number of devices are replaced, the whole production line must be re-deployed and the blockchain must be re-established. This situation will be discussed otherwise. When a comber is successfully registered to the M2M system, the device blockchain will be changed accordingly. Figure 11 shows the information of the new block of the comber after its successful registration.

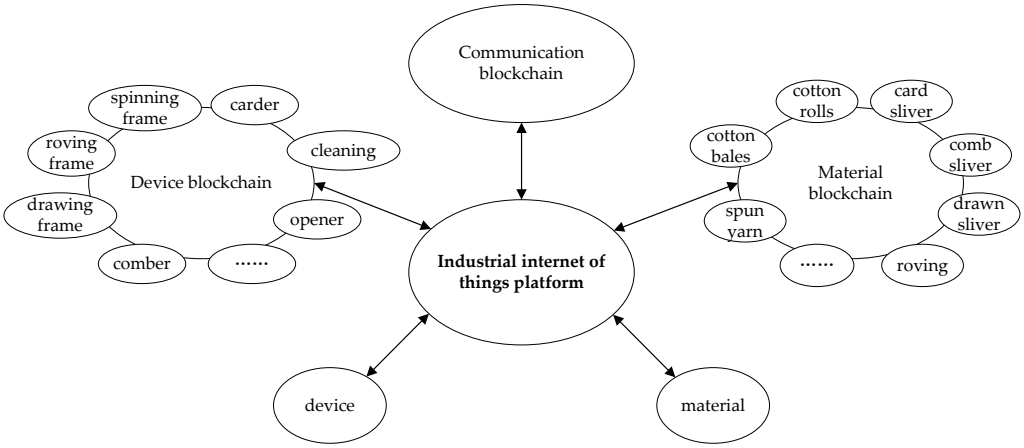

Figure 10. Create device, material, and communication blockchains.

```
                    Successful registration of new device!
New device ID number : D_20160621_1_005
New device name      : drawing frame
New device public key: 02a8aa5451b2f0a1c04d55f94d51f81307d3e713c34afc42e2545d93109d094f94
Registration time    : 2017/5/11 16:50:53
Current block number : 92
```

Figure 11. The information of the new block in a device blockchain.

Furthermore, similar to M2M systems, raw materials are dynamic, as well. That is to say, the forms of materials are different in each step of production. For example, cotton is displayed in bales before opening and cleaning, and roll forms after this step. It will become cotton strips after combing. Cotton is finally presented as spun yarn after all of the processes. The dynamic maintenance of raw materials can also be achieved through blockchain technology. Industrial IoT platforms recognize the IDs of new forms of the material, stamp them with verification time, and then add them to the material blockchain as a new block, as shown in Figure 10. The forms of materials have undergone physical changes in production, but all the transformation data during their entire life cycle are stored in the blockchain. This will be helpful for future data analysis and quality tracing of raw materials and finished yarns. For example, Figure 12 shows that the form of the material in the block is drawn silver.

```
                    The information of new material block
Material origin     : Aksu,xinjiang,China
Material batch      : 1705291
Material form       : drawn sliver
Generation time     : 2017/5/11 19:09:44
Material public key : 024791073d0d372ddf429758bc55c5f3dd0d8214fcc6ebdf4afe823ea38a5a6754
```

Figure 12. The information of the new form of the material in the material blockchain.

From the perspective of the M2M system, the access of a machine does not affect the communication between other devices with the aid of the blockchain, and the security expansion of the devices has been implemented effectively. At the same time, the material blockchain keeps track of the changes of material form, providing guarantee for the production process monitoring and the quality traceability of the material life cycle.

5.2.2. Data Security

In cotton production process, machines, materials, and environment all produce enormous amount of real-time data. Under such large date environments, the request information of any devices in the M2M system, or the operation instructions of the system itself, or how relevant information is transmitted to the target device within the specified time all reflect security and timeliness demand for M2M systems.

As illustrated in Figure 10, all data of machinery and materials in yarn production are stored in the equipment blockchain and raw material blockchain, respectively. If intercommunications happen

between devices or mutual visits occur between equipment and materials, all communication or access process data will be stored in the communication blockchain. At the same time, equipment information of the two communication sides, material information of the accessed materials will be backed up in a timely manner in the communication blockchain. A blockchain has an important feature of keeping multiple backups. If some devices have malfunctions, their own data will, thus, be backed up not only in the device blockchain, but also in its communication blockchain, and in those devices they have been in contact with previously. Even if the IIoT is attacked, it is difficult to tamper with the data due to the existence of multiple copies. All of these ensure the high security and timeliness of data.

Figure 13 shows part of the classes created for the communication objects in our simulations.

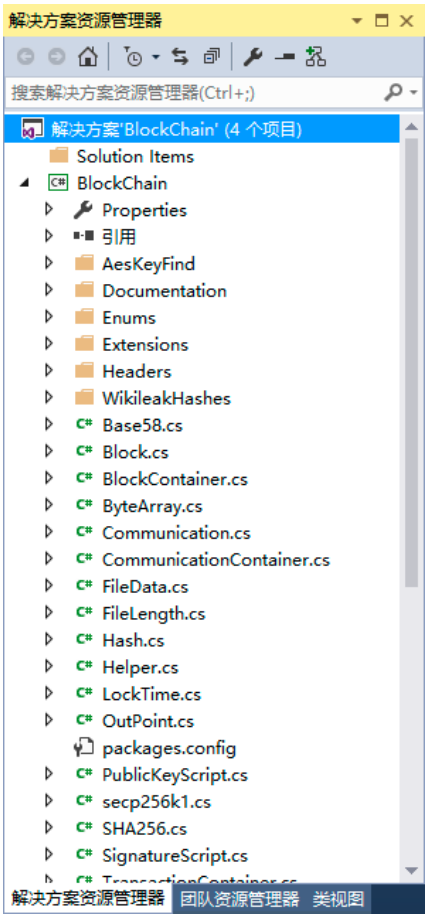

Figure 13. Part of the classes created for the object in the C# environment.

Figure 14 indicates the three cases in which a communication object (a) does not exist, (b) is offline, and (c) is online. Case (a) is that the device has not registered, cannot be accessed and, thus, the communication fails; Case (b) refers to that the device fails to work properly in an offline status, as a result of its maintenance, but its historical data can be accessed from the device blockchain; Case (c) reflects that the device is in the working state and can communicate normally.

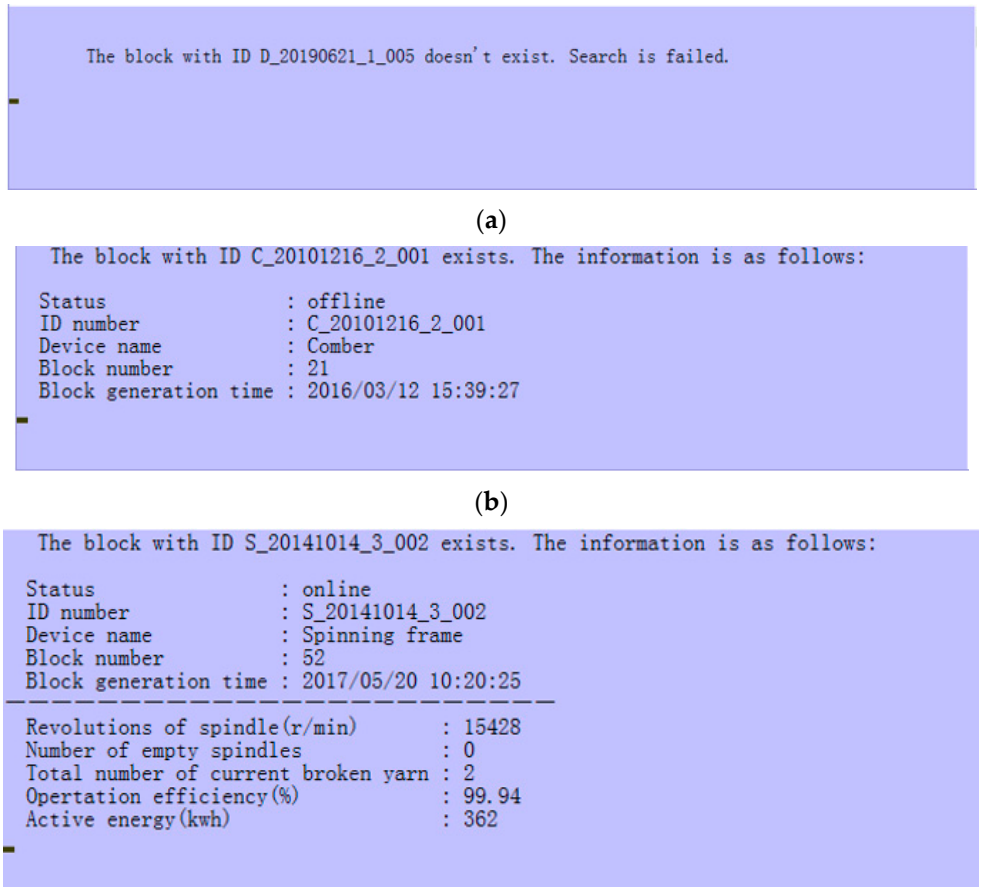

Figure 14. Three cases in which the communication object (**a**) does not exist; (**b**) is offline; and (**c**) is online.

The simulation results of this case study confirm that the device has already left the M2M system, but the data stored in the blockchain can still be accessed, ensuring the communication data is secure.

With the fundamental technology of Bitcoin, the blockchain has gained more and more attention and has begun to be applied to various fields [30], such as medicine [31,32], economics [33,34], the Internet of Things [35,36], and software engineering [37]. We believe that there will be a wide range of applications in M2M security. With the transformation and upgrading of textile enterprises and the expansion of production scale, the update of production equipment will become more frequent. The extensibility of production devices of M2M in CPS will also be challenged. In terms of improving product quality and downgrading production costs, the demand for data of production devices and production processes of textile enterprises is becoming more and more urgent. Therefore, the requirements of data security will increase.

5.2.3. Comparisons

The security of M2M in the existing literature is concentrated in the field of communication. No corresponding countermeasures have been reported to solve the security problems on the M2M of a CPS.

A secure architecture suitable for CPS applications has been presented, which is composed of four layers: a perception layer, a network access layer, data management, and intelligence [21]. This secure architecture can detect black holes, selective forwarding, repetition, delay, data alteration, interference, wormholes, and negligence. Unfortunately, the paper does not present a detailed implementation plan. In contrast, we present our detailed design framework together with the simulation in this

paper. Furthermore, we apply our design of blockchain technology to secure M2M of a CPS for cotton spinning. Our approach differs from existing relevant work on cotton spinning in the following aspects.

First, there are many kinds of devices participating in cotton spinning production. Our model is able to deal with heterogeneous device interconnections. In particular, it can effectively avoid non-interconnection problems caused by the heterogeneity of devices and the amounts of calculation of the communication data encryption by using blockchain technology.

Second, the materials in the production process of cotton spinning always keep changing. For addressing this challenge, we design the material blockchain that can be established to track the changes of the materials and its influence on the product quality.

Finally, during cotton spinning production, the data of the device itself and the data associated with the devices can be lost due to the replacement of devices. Blockchain technology can not only preserve the complete historical data, but also prevent the data from being illegally modified. As such, the data security can be effectively guaranteed.

In summary, our design system on cotton spinning is able to work in a more efficient and secure way.

5.2.4. Outlook on Future Research

First, the data of the devices and the production process are safely stored in the blockchain due to the non-symmetric cryptography principles. With the development of advanced mathematical techniques, the security of the algorithms will, however, become more and more vulnerable. This may cause insecurity with respect to M2M of the CPS because of the blockchain itself. Therefore, the improvement and new development of encryption algorithms to ensure the security of the blockchain is a research direction.

Second, the blockchain technology in this paper was used as a method to study the security of M2M in CPS. This was performed by exploring the security expansion of production devices and data security of M2M communication. We will further explore other security issues of M2M communication of CPS using blockchain technology or other ways to address the M2M security of a CPS.

6. Conclusions

In this paper, we introduced blockchain technology to the security of M2M communication of a CPS. The main features and working principles of a blockchain were described. According to the characteristics and principles of a blockchain, we have presented a design of a blockchain for M2M communication security of a CPS. As is known, an M2M communication system consists of three areas—public networks area, device areas, and private areas. We presented our design of the structures of the machine and equipment blockchain in the public network area, as well as the communication blockchain in the private area in detail. Using a case study on cotton spinning production, we have demonstrated that blockchain technology can safely expand machines and secure the communication of data between them in the cotton production process.

Acknowledgments: This study was supported by the Fundamental Research Funds for the Central Universities, China, and the National Natural Science Foundation of China (51475301 and 61370229).

Author Contributions: Shiyong Yin and Jinsong Bao conceived this study and wrote the paper; Yiming Zhang conceived and designed the case study; Xiaodi Huang performed the case study and wrote the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Park, K.J.; Zheng, R.; Liu, X. Cyber-physical systems: Milestones and research challenges. *Comput. Commun.* **2012**, *36*, 1–7. [CrossRef]
2. Palavicini, G., Jr.; Bryan, J.; Sheets, E.; Kline, M.; Miguel, J. Towards firmware analysis of industrial internet of things (IIoT)—Applying symbolic analysis to IIOT firmware vetting. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 24–26 April 2017; pp. 470–477.

3. Kim, B.H.; Ahn, H.J.; Kim, J.O.; Yoo, M. Application of M2M technology to manufacturing systems. In Proceedings of the International Conference on Information and Communication Technology Convergence, Jeju, Korea, 17–19 November 2010; pp. 519–520.
4. Burmester, M.; Magkos, E.; Chrissikopoulos, V. Modeling security in cyber–physical systems. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 118–126. [CrossRef]
5. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
6. Wang, E.K.; Ye, Y.M.; Xu, X.F.; Yiu, S.M.; Hui, C.K.; Chow, K.P. Security issues and challenges for cyber physical system. In Proceedings of the IEEE/ACM International Conference on Green Computing and Communications & Cyber, Physical and Social Computing, Hangzhou, China, 18–20 December 2010; pp. 733–738.
7. Djenouri, D.; Khelladi, L.; Badache, A.N. A survey of security issues in mobile ad hoc and sensor networks. *IEEE Commun. Surv. Tutor.* **2005**, *7*, 2–28. [CrossRef]
8. Anand, M.; Cronin, E.; Sherr, M.; Blaze, M.; Ives, Z.; Lee, I. Security challenges in next generation cyber physical systems. In Proceedings of the Beyond SCADA: Network Embedded Control for Cyber Physical Systems, Washington, DC, USA, 16–17 March 2006.
9. Lee, E.A. Cyber physical systems: Design challenges. In Proceedings of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing, Washington, DC, USA, 5–7 May 2008; pp. 363–369.
10. Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.
11. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [CrossRef]
12. Xu, Q.; Ren, P.Y.; Song, H.B.; Du, Q.H. Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions. *IEEE Int. Things J.* **2017**. [CrossRef]
13. Medaglia, C.; Serbanati, A. An overview of privacy and security issues in the internet of things. In Proceedings of the 20th Tyrrhenian International Work-Shop on Digital Communications, Sardinia, Italy, 18–20 September 2009; pp. 389–395.
14. Weber, R. Internet of things-new security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *6*, 23–30. [CrossRef]
15. Saedy, M.; Mojtahed, V. Ad hoc M2M communications and security based on 4G cellular system. *Wirel. Telecommun. Symp.* **2011**, 1–5. [CrossRef]
16. Tuna, G.; Kogias, D.G.; Gungor, V.C.; Gezer, C.; Taşkın, E.; Ayday, E. A survey on information security threats and solutions for machine to machine (M2M) communications. *J. Parallel Distrib. Comput.* **2017**, *109*, 142–154. [CrossRef]
17. Chen, S.; Ma, M.D. A dynamic-encryption authentication scheme for M2M security in cyber-physical systems. In Proceedings of the Global Communications Conference, Atlanta, GA, USA, 9–13 December 2013; pp. 2897–2901.
18. Inhyok, C.; Shah, Y.; Schmidt, A.U.; Leicher, A.; Meyerstein, M.V. Trust in M2M communication. *IEEE Veh. Technol. Mag.* **2009**, *4*, 69–75.
19. He, Y.Y.; Chen, L.Q.; Wang, L.L. An improved direct anonymous attestation scheme for M2M network. *Proced Eng.* **2011**, *15*, 1481–1486. [CrossRef]
20. Zhang, K.S.; Chen, M.Z. Research of environment monitoring platform of mine area based on M2M. *Ind. Mine Autom.* **2013**, *39*, 63–67.
21. Chen, D.; Chang, G.R. A survey on security issues of M2M communications in cyber-physical systems. *KSII Trans. Internet Inf. Syst.* **2012**, *6*, 24–45. [CrossRef]
22. Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient adaptive resource management for real-time vehicular cloud services. *IEEE Trans. Cloud Comput.* **2016**. [CrossRef]
23. Javanmardi, S.; Shojafar, M.; Shariatmadari, S.; Ahrabi, S.S. Fr Trust: A fuzzy reputation based model for trust management in semantic P2P grids. *Int. J. Grid Util. Comput.* **2015**, *6*, 57–66. [CrossRef]
24. Du, Q.H.; Li, W.Y.; Song, H.B. Security enhancement via dynamic fountain code for wireless multicast. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications, Guilin, China, 27 May 2017; pp. 509–521.

25. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 12 August 2017).
26. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media: Sebastopol, CA, USA, 2015.
27. Yuan, Y.; Wang, F.Y. Blockchain: The state of the art and future trends. *ACTA Autom. Sin.* **2016**, *42*, 481–494.
28. Appel, A.W. Verification of a cryptographic primitive: Sha-256. *ACM Trans. Program. Lang. Syst.* **2015**, *37*, 7. [CrossRef]
29. Fan, S.Q.; Wang, W.B.; Cheng, Q.F. Attacking openssl implementation of ECDSA with a few signatures. In Proceedings of the ACM Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1505–1515.
30. Li, X.Q.; Jiang, P.; Chen, T.; Luo, X.P.; Wen, Q.Y. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2017**, in press, accepted manuscript. [CrossRef]
31. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2nd International Conference on Open and Big Data, Vienna, Austria, 25–30 August 2016.
32. Yue, X.; Wang, H.J.; Jin, D.W.; Li, M.Q.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef] [PubMed]
33. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of things, blockchain and shared economy applications. *Proced Comput. Sci.* **2016**, *98*, 461–466. [CrossRef]
34. Hurich, P. The virtual is real: An argument for characterizing bitcoins as private property. *Bank. Financ. Law Rev.* **2016**, *31*, 573.
35. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IOT security and privacy: The case study of a smart home. In Proceedings of the 2nd IEEE Percom Workshop on Security Privacy and Trust in the Internet of Things, Hawaii, HI, USA, 13–17 March 2017.
36. Zhang, Y.; Wen, J. The IOT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2016**, *10*, 1–12. [CrossRef]
37. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.B.; Chen, S. The blockchain as a software connector. In Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture, Venice, Italy, 5–8 April 2016.